REMARKS

Applicants are herewith filing an RCE to continue the prosecution of this application. This Amendment is being filed to respond to the rejections of the claims given in the Office Action of December 6, 2005.

In that Office Action, the Examiner rejected Claims 1-5, 7-9, 11-13, 15 and 16, which are all of the pending claims, under 35 U.S.C. 112, first paragraph, and under 35 U.S.C. 103 as being unpatentable over the prior art. More specifically, Claims 1-5, 7-9, 11-13, 15 and 16 were rejected under 35 U.S.C. 112 on the basis that the specification does not support the limitation that an encrypted copy of the unsigned coin is sent back to the user, and that the specification does not enable the limitation that both an encrypted copy of the signed coin and an encrypted copy of the unsigned coin are sent back to the user.

With respect to the rejection of the claims under 35 U.S.C. 103, Claims 1, 2, 15 and 16 were rejected as being unpatentable over U.S. Patent 6,311,171 (Dent) in view of U.S. Patent 6,298,153 (Oishi); and Claims 3-5, 7-9 and 11-13 were rejected as being unpatentable over U.S. Patent 5,832,089 (Kravitz, et al.) in view of Oishi.

The rejections of the claims under 35 U.S.C. 112 are respectfully traversed. Also, Applicants herein ask that independent Claims 1, 3, 7 and 11 be amended to better define the subject matters of these claims.

For the reasons set forth below, Claims 1-5, 7-9, 11-13, 15 and 16 comply with the requirements of 35 U.S.C. 112 and also patentably distinguish over the prior art and are allowable. The Examiner is thus asked to reconsider and to withdraw the rejections of Claims 1-5, 7-9, 11-13, 15 and 16 under 35 U.S.C. 103 and 112, and to allow these claims.

8

BEST AVAILABLE COPY

This invention relates to the creation and use of electronic cash. In accordance with a preferred embodiment of the invention, a customer sends a request for digital cash to a bank, along with a public key of an encryption scheme. The bank signs the cash using a secret key of a digital signature scheme, and encrypts the signature by using the public key provided by the customer. The bank also encrypts an unsigned copy of the cash, and the bank sends back to the customer a copy of the encrypted signed cash and a copy of the encrypted unsigned cash.

The customer then decrypts both the signed and unsigned copies of the cash by using the private key of the encryption scheme, and the customer then uses this signed and unsigned pair of copies for payment to a third party. The third party, using the signed and unsigned copies of the cash, can then ask the bank to confirm the validity of the digital cash, and if that validity is confirmed, this third party is able to redeem the digital cash for payment.

As indicated above, in rejecting the pending claims under 35 U.S.C. 112, the Examiner argued that the specification does not support the limitation that an encrypted copy of the unsigned coin is sent back to the user, and that the specification does not enable the limitation that both an encrypted copy of the signed coin and an encrypted copy of the unsigned coin are sent back to the user.

These aspects of the invention are discussed at several places in the specification. It may be helpful to note that in these discussion, the coin is referred to as "Unit," and the signed copy of the coin is referred to as "Sign(Unit)." Also, the encrypted unsigned copy is "Encr2(Unit) and the encrypted signed copy of the coin is "Encr2(Sign)(Unit)).

As explained on pages 9 and 10 of the specification, each unit (Unit) is signed by the secure cryptography generator. The signature is then encrypted by using the customer's public encryption scheme. Further, as mentioned on page 10, line 4, the secure cryptography

9

G:\IBM\105\13879\amend\13879.am8.doc

BEST AVAILABLE COPY

generator also encrypts the unsigned unit (Unit). It is then explained on page 10, that, among other values, the encrypted singed unit (Encr2(Sign1(Unit))) and the encrypted unsigned unit (Encr2(Unit)) are both sent to the computer system of the bank, and then to the customer C.

In view of the above-remarks and the associated description in the specification, it is believed that the specification discloses, fully enables and explains how the encrypted copy of the signed coin and the encrypted copy of the unsigned coin are formed and used in the present invention. The Examiner is, accordingly, respectfully asked to reconsider and to withdraw the rejections of Claims 1-5, 7-9, 11-13, 15 and 16 under 35 U.S.C. 112.

Further, the use of this pair of copies of the coin - encrypted copies of the signed and unsigned coin sent to the customer - is an important distinction between the present invention and the prior art. With these two copies, a third party can readily determine the amount of the coin without decoding the signed copy, and this third party can, by using the signed copy, conform that amount with the bank before accepting payment. The prior art of record does not disclose or suggest the use of these two copies of the coin.

For instance, Dent discloses a procedure for providing secure electronic communications. In this procedure, coins are encrypted by a bank using the owner's secret key. The encrypted coins are sent back to the owner, who can decrypt them using a public key and then can use the coins as payment.

Kravitz, et al. describes a procedure for handling electronic cash. With this procedure, a customer is provided with encrypted copies of a signed and unsigned coin. These are decrypted by the customer using a secret key, and the decrypted signed unit can then be used as a payment.

As the Examiner has recognized, there are a number of important features of the present invention that are not shown in or suggested by either Dent or Kravitz, et al.

10   G:\IBM\105\13879\amend\13879.am8.doc

BEST AVAILABLE COPY

One important feature of the present invention that is not shown in either of these references is the use by the owner of the pair of signed and unsigned coins as payment to a recipient or third party.

Oishi also does not show or suggest this feature of the invention. Oishi discloses several digital signature procedures, including the use of an anonymous public key certificate. Non-homomorphic signature schemes, per se, are know. Significantly, Oishi does not relate to digital cash, and does not provide any suggestion or guidance as to how to use effectively the disclosed cryptographic methods in a digital cash system. Moreover, Oishi clearly does not address the same specific problem - providing secure digital cash that can be used by a customer in a conventional manner while still maintaining the customer's identity anonymous to the bank - that is effectively addressed by the present invention.

The Examiner, in the Office Action, cited specific portions of Oishi as allegedly disclosing the feature of sending back to a user encrypted copies of both a signed coin and an unsigned coin. In particular, the Examiner cited column 11, lines 48-54 of Oishi. This section of Oishi describes a certificate publisher terminal device that has a public key generating unit and a signature-generating unit. There is no teaching in this portion of Oishi, or anywhere else in this reference, of encrypting both signed and unsigned copies of a coin, yet alone of using these encrypted copies in the manner in which they are used in the present invention.

Applicants herein ask that independent Claims 1, 3, 7 and 11 be amended to describe the above-discussed feature of this invention. In particular, Claims 1 and 7, as amended herein, describe the features that the user or the customer uses the private key to decrypt both the signed and unsigned copies of the coin and uses that pair of coins - that is, the signed and unsigned copies of the coin - as digital cash. Claim 7 add the further limitation that this pair

11

G:\IBM\105\13879\amend\13879.am8.doc

BEST AVAILABLE COPY

of coins is used as a payment to a recipient. Claims 3 and 11, as amended herein, describe the features that the pair of decrypted coins - the signed and unsigned copies - are used as a unit as payment to a recipient, and that this recipient then presents this pair of coins to the bank for credit.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, also do not disclose or suggest this use of the pair of decrypted signed and unsigned coins, as described in Claims 1, 3, 7 and 11.

In light of the differences between Claims 1, 3, 7 and 11 and the prior art, and because of the advantages associated with those differences, these claims patentably distinguish over the prior art and are allowable. Claim 2 is dependent from Claim 1 and is allowable therewith; and Claims 4, 5, 15 and 16 are dependent from Claim 3 and are allowable therewith. Likewise, Claims 8 and 9 are dependent from Claim 7 and are allowable therewith; and Claims 12 and 13 are dependent from, and are allowable with, Claim 11.

For the reasons discussed above, the Examiner is asked to reconsider and to withdraw the rejections of Claims 1-5, 7-9, 11-13, 15 and 16 under 35 U.S.C. 103 and 112, and to allow these claims. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,

John S. Sensny
Registration No. 28,757
Attorney for Applicants

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza - Suite 300
Garden City, New York 11530
(516) 742-4343
JSS:jy

12

G:\IBM\105\13879\amend\13879.am8.doc